IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

MARKING OBJECT VIRTUALIZATION INTELLIGENCE, LLC, ***Plaintiff,*** v. **HEWLETT PACKARD ENTERPRISE COMPANY; HP ENTERPRISE SERVICES, LLC; F5 NETWORKS, INC.; AND TREND MICRO, INC.** ***Defendants.***	**Civil Action No._____** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Marking Object Virtualization Intelligence, LLC ("MOV Intelligence" or "Plaintiff"), by and through its attorneys, brings this action and makes the following allegations of patent infringement relating to U.S. Patent Nos.: 7,200,230 ("the '230 patent"); 6,802,006 ("the '006 patent"); 6,510,516 ("the '516 patent"); 7,650,504 ("the '504 patent"); 7,650,418 ("the '418 patent") and 7,124,114 ("the '114 patent") (collectively, the "patents-in-suit" or the "MOV Intelligence Patents"). Hewlett Packard Enterprise Company ("HPEC") and HP Enterprise Services, LLC ("HPES") (collectively, "HPE") infringe the '230, '006, '516, and '504 patents. HPE and F5 Networks, Inc. ("F5 Networks") jointly infringe the '418 patent. HPE and Trend Micro, Inc. ("Trend Micro") infringe the '114 patent. Defendants HPEC, HPES, F5 Networks, and Trend Micro's (collectively, the "Defendants") infringement violates the patent laws of the United States of America, 35 U.S.C. § 1 *et seq*.

INTRODUCTION

1. MOV Intelligence and its wholly-owned subsidiary, MOV Global Licensing LLC ("MOV Global Licensing") pursue the reasonable royalties owed for Defendants' unauthorized use of patented groundbreaking technology both here in the United States and throughout Europe.

2. Rovi Corporation ("Rovi") [1] is a pioneer and leader in protecting computer technology, including digital rights management ("DRM") and digital watermarking systems. Rovi assigned MOV Intelligence rights to over 233 patents including many of John O. Ryan's, the founder of Rovi predecessor Macrovision, groundbreaking patents.[2]

3. The patents-in-suit, their underlying patent applications, and foreign counterparts have been cited by over 450 issued United States patents and published patent applications. HPE has referenced the patents-in-suit in 8 issued patents and published patent applications as relevant prior art.

- U.S. Patent No. 7,961,879 (citing the '230 patent and assigned to HPE subsidiary Voltage Security, Inc.)
- U.S. Patent No. 7,580,521 (citing the '230 patent and assigned to HPE subsidiary Voltage Security, Inc.)
- U.S. Patent No. 7,558,954 (citing the '230 patent and assigned to Hewlett-Packard Development Company, L.P.)
- WO/2005045653A1 (citing the '230 patent and assigned to Hewlett-Packard Development Company L.P.)
- U.S. Patent App. No. 2007/0220500 (citing the '006 patent and assigned to Hewlett-Packard Development Company, L.P.)
- U.S. Patent No. 8,051,299 (citing the '006 patent and (citing the '006 patent and assigned to Hewlett-Packard Development Company, L.P.)
- U.S. Patent App. No. 2004/0086125 (citing the '114 patent and assigned to Hewlett-Packard Development Company, L.P.)
- U.S. Patent No. 7,415,113 (citing the '114 patent and assigned to Hewlett-Packard Development Company, L.P.)

[1] On April 29, 2016, Rovi Corporation acquired TiVo, Inc. The combined company operates under the name TiVo, Inc.

[2] *See* U.S. Patent Nos. 6,381,367; 7,764,790; 6,701,062; 8,014,524; German Patent Nos. DE60001837 and DE60001837D1; Chinese Patent No. CN1186941C; Canadian Patent No. CA2379992C; European Patent No. EP1198959B1; and Japanese Patent No. JP4387627B2.

THE PARTIES

MARKING OBJECT VIRTUALIZATION INTELLIGENCE, LLC

4. Marking Object Virtualization Intelligence, LLC ("MOV Intelligence") is a Texas limited liability company with its principal place of business located at 903 East 18th Street, Suite 217, Plano, Texas 75074. MOV Intelligence is committed to advancing the current state of DRM and watermarking technologies.

5. MOV Intelligence Global Licensing, LLC ("MOV Global Licensing") is a wholly-owned subsidiary of MOV Intelligence and assists in the licensing of MOV Intelligence's patents in territories outside the United States with a focus on the European Union (and the United Kingdom).[3] MOV Intelligence Global Licensing, LLC is a corporation organized under the laws of Delaware.

6. Rovi assigned the following patents to MOV Intelligence: U.S. Patent Nos. 7,299,209; 6,510,516; 6,802,006; 7,650,504; 6,813,640; 7,650,418; 7,200,230; 7,124,114; 6,381,367; 6,374,036; 6,360,000; 6,553,127; 6,701,062; 6,594,441; 7,764,790; 8,014,524; 6,931,536; and International Patent Nos. DE60047794; DE60148635.8; DE60211372.5; DE69901231.7-08; DK1047992; EP1047992; EP1303802; EP1332618; EP1444561; ES1047992; FR1047992; FR1303802; FR1332618; FR1444561; GB1047992; GB1303802; GB1332618; GB1444561; GR3040059; IE1047992; IE1444561; IT1047992; NL1047992; NL1444561; PT1047992; and SE1047992.

7. MOV Intelligence has the right to sublicense the following international patent assets held by Rovi: AT1020077; AT1198959; AT1080584; ATE232346; AT1020077; AU729762; AU741281; AU753421; AU743639; AU714103; AU729762; AU2002351508; AU765747; AU2000263715; BE1020077; BE1198959; BE1020077; BE1080584; BE900498; BRPI 9812908-2; BR9709332.7; BRPI 9812908-2; CA2305254; CA2332546; CA2379992; CA2305254; CA2332548; CA2557859; CA2252726; CA2462679; CA2315212; CA2416304; CA2425115; CH1020077; CH1080584; CH900498; CH1020077; CH1047992;

[3] Wolfram Schrag, *EU-Patent steht auf der Kippe*, BR.COM NACHRICHTEN (August 2016).

CNZL98809610.2; CNZL99806376.2; CNZL00811179.0; CNZL98809610.2; CNZL99806377.0; CNZL97194746.5; CNZL02820738.6; CNZL99802008.7; CNZL00819775.X; CNZL200510089437; DE69807102.608; DE60001837.7; DE69908352.4-08; DE69718907.4-08; DE69807102.608; DK1020077; DK1080584; DK1198959; DK1020077; DK900498; EP1020077; EP1198959; EP1080584; EP900498; EP1020077; ES1020077; ES1198959; ES1080584; ESES2191844; ES1020077; FI1020077; FI1080584; FI1020077; FI900498; FR1020077; FR1198959; FR1080584; FR900498; FR1020077; GB1020077; GB1198959; GB1080584; GB900498; GB1020077; GR3041381; GR3045620; GR3043304; GR3041381; HK1028696; HKHK1035625; HK1028696; HK1035282; HK1018562; HKHK1069234; HKHK1057115; HK1083653B; IE1020077; IE1198959; IE1020077; IE1080584; IE900498; IL135498; IL139543; IL148002; IL135498; IL139544; IN201442; IN220504; IN201442; IN207829; IT1020077; IT1080584; IT900498; IT1020077; JP4139560; JP4263706; JP4387627; JP4551617; JP4139560; JP4263706; JP3542557; JP4627809; JP4698925; JP4366037; JP4307069; KR374920; KR422997; KR761230; KR374920; KR362801; KR478072; KR689648; KR539987; KR752067; KR728517; KR593239; MX223464; MX231725; MX226464; MX223464; MX212991; MX214637; MX237690; MX240845; MYMY-123159-A; MYMY-123159-A; NL1020077; NL1198959; NL1080584; NL900498; NL1020077; NZ503280; NZ507789; NZ503280; NZ532122; PT1010077; PT1198959; PT1080584; PT900498; PT1010077; RU2195084; RU2216121; RU2251821; RU2195084; RU2208301; RU2258252; SE1020077; SE1198959; SE1080584; SE900498; SE1020077; SG71485; SG76965; SG86547; SG76964; SG71485; TWNI117461; TWNI-124303; TWNI-130428; TWNI1600674; TWNI-162661; TWNI-202640; TWNI117461; TWNI-130754; and TWNI-184111.

HEWLETT PACKARD ENTERPRISE COMPANY & HP ENTERPRISE SERVICES, LLC

8. On information and belief, Hewlett Packard Enterprise Company is a Delaware corporation with its principal place of business at 3000 Hanover Street, Palo Alto, California

94304. HPE may be served through its registered agent 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

9. On information and belief, HPEC is registered to do business in the State of Texas.

10. On information and belief, HPEC conducts business operations throughout the State of Texas, and within the Eastern District of Texas, in facilities in Houston and Plano, Texas.

11. On information and belief, HP Enterprise Services, LLC is a Delaware limited liability company having a principal place of business at 5400 Legacy Drive, Plano, Texas 75024. On information and belief, HPES can be served through its registered agent, CT Corporation System, 1999 Bryan St., Ste. 900, Dallas, Texas 75201.

12. HPES maintains a campus in Plano Texas that consists of 3,521,000 square feet (327,100 m^2) of office and data center space on 270 acres (1.1 km^2) of land. *See Abstrax, Inc. v. Hewlett-Packard Co.*, Case No. 14-cv-158 Dkt. No. 86 (E.D. Tex. Nov. 11, 2014) (finding significant ties to the district including 5,000 HP employees located in the district at HP's Plano, Texas facility); *Mirror Worlds Techs., LLC v. Dell Inc., et al.*, Case No. 13-cv-00941 Dkt. No. 179 (E.D. Tex. Sept. 29, 2014) (denying HP's motion to transfer venue and concluding that HP [along with other defendants] collectively employ thousands of people in or near the Eastern District of Texas).

F5 NETWORKS, INC.

13. On information and belief, Defendant F5 Networks, Inc. ("F5 Networks") is a Washington corporation with a principal office located at 401 Elliott Avenue West, Seattle, WA 98119. F5 Network's registered agent in Texas appears to be CT Corporation System, 350 N St. Paul St., Suite 2900, Dallas, Texas 75201.

14. On information and belief, F5 Network is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at

least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

HPE AND F5 NETWORKS JOINT SOLUTION - HPE ATALLA HSM WITH F5 BIG-IP LTM

15. On information and belief, HPE and F5 Networks, in a joint enterprise, design, make, sell, offer to sell, import, and/or use a joint solution, the HPE Atalla HSM and F5-BIG IP Local Traffic Manager solution ("HPE-HSM F5-LTM product"). HPE and F5 Networks describe HPE-HSM F5-LTM as being a "joint solution." "[T]he advantages of the ***joint solution of HPE Atalla HSM and F5-BIG IP Local Traffic Manager (LTM)*** to provide data security, scalable, and high availability deployment."[4]

16. HPE and F5 Network executives have described the HPE-HSM F5-LTM product as coming out of their joint collaboration. "HP and F5 are collaborating on an SDN application called the DDOS Umbrella. And also on the integration of our BIG-IP product and our intelligent management center management product."[5]

17. F5 claims on its website that the joint solution provides a "fluid and responsive infrastructure."

> F5 Application Delivery Controllers provide strategic points of control in the data center, ensuring high availability, accelerated applications, and enhanced security. When F5 solutions are combined with HPE Software, customers can achieve a fluid and responsive infrastructure that aligns IT—including virtualization, automation, and security strategies—to constantly changing business needs.

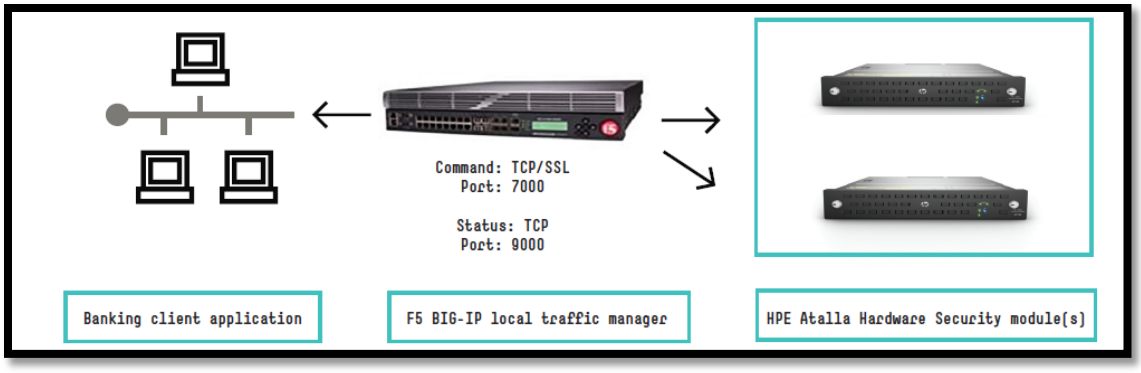
HPE-F5 Technology Alliance Webpage, F5 NETWORKS WEBSITE (last visited September 2016), available at: https://f5.com/solutions/technology-alliances/hpe

[4] *Network and data security solution with F5 BIG-IP LTM*, HPE SOLUTION BRIEF at 1 (May 2016) (emphasis added).

[5] Dominic Wilde (Vice President at HPE), *Transcript of Presentation from HP and F5 Working Together*, AGILITY CONFERENCE 2014 (August 2014), available at: https://www.youtube.com/watch?v=u6Y5vR0NJ0s

18. On information and belief, HPE and F5 Networks offer the HPE-HSM F5-LTM product based on contractual agreements between HPE and F5 Networks. "HP's partnership with F5 Networks (the undisputed ADC market share leader) provides customers with an industry-leading value proposition focused on addressing mission-critical application performance demands, virtualized data centers, and cloud services."[6]

19. The following diagram from HPE shows an exemplar implementation of the HPE-HSM F5-LTM product.



Network and Data Security Solution with F5 BIG-IP LTM, HPE SOLUTION BRIEF at 2 (May 2016).

TREND MICRO, INC.

20. On information and belief, Trend Micro, Inc. is a California corporation, with its headquarters at 225 E. Johnson Carpenter Freeway, Suite 1500, Irving, Texas 75062. On information and belief, Trend Micro can be served through its registered agent, Ruth Ann Roman, 225 E. Carpenter Freeway, Suite 1500, Irving, Texas 75062.

21. On information and belief, Trend Micro's infringing products are offered for sale and sold throughout the United States, including in this District, through various channels. Trend Micro offers its infringing products through its distribution channel, which includes numerous distribution points in Texas. Further, Trend Micro advertises its infringing products throughout the Eastern District of Texas.

[6] *HP FlexFabric Reference Architecture Overview*, HP TECHNICAL WHITEPAPER at 10 (2012).

THE TREND MICRO-HPE PRODUCT - TIPPINGPOINT SECURITY MANAGEMENT SYSTEM

22. HPE and Trend Micro make, sell, offer to sell, import, and/or use TippingPoint Security Management Systems (SMS) that infringe the '114 patent. HPE's infringing products include: HP Security Management System H3 Appliance, HP Security Management System H3 XL Appliance, and HP vSMS Essential for VMware (collectively, the "HPE TippingPoint product(s)"). Trend Micro's infringing products include: Trend Micro TippingPoint Security Management System H3 Appliance, Trend Micro TippingPoint Security Management System H3 XL Appliance, Trend Micro TippingPoint vSMS Essential Virtual Appliance, and Trend Micro TippingPoint vSMS Enterprise Virtual Appliance (collectively, the "Trend Micro TippingPoint product(s)").

23. The HPE TippingPoint products and Trend Micro TippingPoint products (collectively, the "HPE-Trend Micro TippingPoint product(s)"), are security management systems that provide policy-based security management for networks.

24. In October 2015, Trend Micro acquired HPE's TippingPoint technologies.[7] Subsequently, HPE TippingPoint products were rebranded as Trend Micro TippingPoint products. HPE and Trend Micro have stated that the TippingPoint products remained the same between when they were sold by HPE and now that they are sold by Trend Micro.[8] "While TippingPoint is now part of the Trend Micro family, there are no plans to change any of TippingPoint's award-winning services."[9]

[7] *Trend Micro Acquires HP TippingPoint, Establishing Game-Changing Network Defense Solution*, TREND MICRO PRESS RELEASE (October 21, 2015), available at: http://newsroom.trendmicro.com/press-release/company-milestones/trend-micro-acquires-hp-tippingpoint

[8] *HPE ArcSight Connector Supported Products*, HPE DATA SHEET at 2 (July 2016).

[9] Jon Dykes, TREND MICRO LETTER TO TIPPINGPOINT CUSTOMERS at 1 (March 9, 2016).

25. HPE and Trend Micro partnered to develop the infringing HP-Trend Micro TippingPoint products. "HPE has partnered with Trend Micro, an industry leader in advanced persistent threat detection, to create the HPE TippingPoint ATA family."[10]

26. Trend Micro and HPE have entered into licensing and technology agreements that govern the development and sale of the HPE-Trend Micro Products. "The two companies will form a strategic partnership with TippingPoint around re-sale, managed services and OEM activities, as well as security intelligence, app security and data security."[11]

27. Even prior to Trend Micro's acquisition of the HPE TippingPoint products, HPE had entered into licensing agreements with Trend Micro that governed the sale of the TippingPoint products. "The HP TippingPoint Advanced Threat Appliance includes Trend Micro Software which is licensed in accordance with the terms and conditions located at www.trendmicro.com/cloud-content/us/pdfs/eula/en-_english_multicountry_-_smb-enterprise_eula__dec_2014_.pdf."[12]

28. On information and belief, HPE and Trend Micro are not direct competitors. HPE and Trend Micro have described their relationship as being a "strategic partner[ship]." "Since 2014, Trend Micro and TippingPoint have had a strategic partner relationship. HP and Trend Micro will continue to be strong partners post transaction."[13]

29. As of October 6, 2016, HPE continues to provide extensive product materials relating to the HPE-Trend Micro TippingPoint products including providing customers with

---

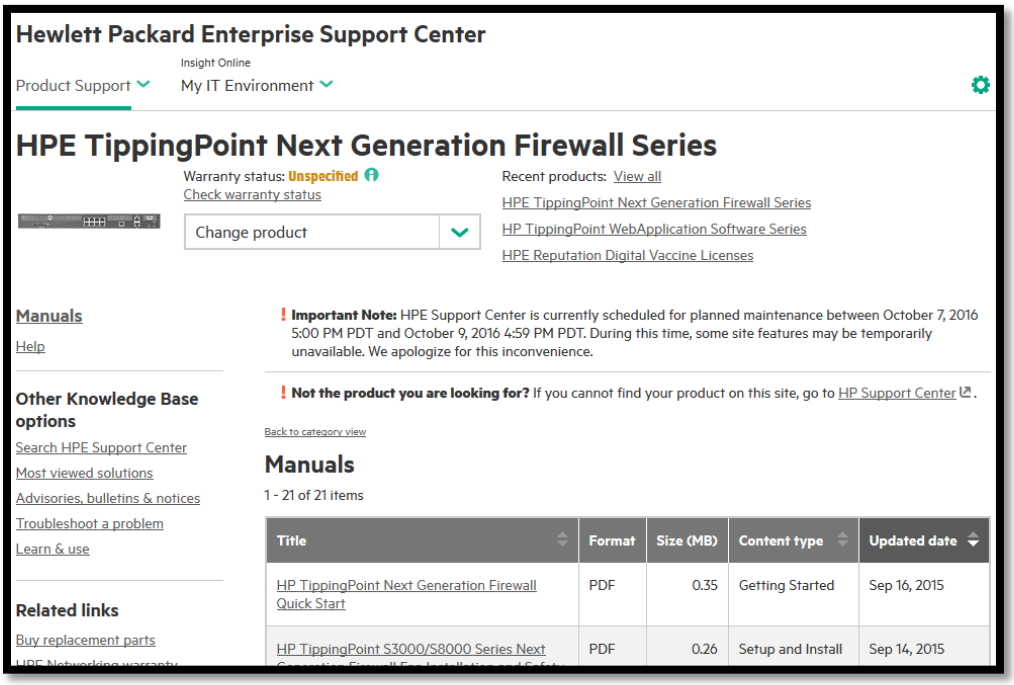
[10] *HPE TippingPoint Advanced Threat Appliance Family*, HPE DATA SHEET at 2 (November 2015).

[11] *Trend Micro Acquires HP TippingPoint, Establishing Game-Changing Network Defense Solution*, TREND MICRO PRESS RELEASE (October 21, 2015), available at: http://newsroom.trendmicro.com/press-release/company-milestones/trend-micro-acquires-hp-tippingpoint

[12] *HP TippingPoint Products Additional License Authorizations*, HPE LICENSING DOCUMENTS (May 2014).

[13] *Trend Micro Acquires HP TippingPoint, Establishing Game-Changing Network Defense Solution*, TREND MICRO PRESS RELEASE (October 21, 2015), available at: http://newsroom.trendmicro.com/press-release/company-milestones/trend-micro-acquires-hp-tippingpoint

drivers and software updates, manuals, and getting started guides. HPE makes these materials available through the Hewlett Packard Enterprise Support Center. The below screenshot of the HPE Support Center website shows HPE's continuing support of HPE TippingPoint products.



HPE TippingPoint Next Generation Firewall Series, HEWLETT PACKARD ENTERPRISE SUPPORT CENTER (last visited October 6, 2016), available at: http://h20565.www2.hpe.com/portal (screenshot showing HPE's continued support for HPE TippingPoint products).

30. On information and belief, the sale of the infringing HPE TippingPoint products and Trend Micro TippingPoint products has occurred during the same time period. Specifically, HPE and Trend Micro's sold HPE-Trend Micro TippingPoint products at the same time.

31. On information and belief, the HPE TippingPoint products and Trend Micro Tipping Point products use identical components. Specifically, the HPE and Trend Micro products use the same computer code and were developed by the same individuals.

32. Joinder of HPE and Trend Micro in this case is appropriate under U.S.C. 35 § 299 given questions of fact are common among both Defendants, including: Defendants' infringement of the '114 patent stems from the manufacture and distribution of the same product, licensing and technology agreements between Trend Micro and HPE, the longstanding relationship between HPE and Trend Micro, and the alleged acts of infringement occurred and

continue to occur in the same time period. *See In re EMC* Corp., 677 F.3d 1351, 1359-60 (Fed. Cir. 2012).

33. The shared overlapping facts that give rise to Trend Micro and HPE's infringement of the '114 patent "constitutes a series of transactions" that make joinder appropriate. *See MGT Gaming, Inc. v. WMS Gaming, Inc.*, 978 F. Supp. 2d 647, 660 (S.D. Miss. 2013) (finding joinder appropriate where there was an ongoing relationship to split revenues); *Smartflash LLC v. Apple, Inc.*, No. 6:13-cv-447, 2014 U.S. Dist. LEXIS 185268, at *11-12 (E.D. Tex. Apr. 4, 2014) (finding joinder proper where there was a logical relationship between "three developers" that all used the same development framework to "develop their infringing in-app functionality").

JURISDICTION AND VENUE

34. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

35. Upon information and belief, this Court has personal jurisdiction over Defendants in this action because Defendants have committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Defendants would not offend traditional notions of fair play and substantial justice. Defendants, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit.

36. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Defendants have transacted business in the Eastern District of Texas and have committed acts of direct and indirect infringement in the Eastern District of Texas.

MOV INTELLIGENCE'S LANDMARK INVENTIONS

37. The groundbreaking inventions in DRM and digital watermarking taught in the patents-in-suit were pioneered by Rovi. Rovi, established in 1983 under the name Macrovision, was a trailblazing technology company focused on inventing and bringing to market fundamental technologies designed to allow producers and distributors of film and music to widely distribute their products while simultaneously protecting their art from unauthorized copying.[14] Macrovision's copy protection technology became so important to content creators that Congress specifically regulated the manufacture and sale of technology that was incompatible with Macrovision's copy protection technology. *See* 17 U.S.C. § 1201(k)(1) ("unless such recorder conforms to the automatic gain control copy control technology").[15] Rovi broadened its focus to include copy protection and DRM for other media,[16] including computer executables, firmware, operating system images, watermarking, and encryption.

38. MOV Intelligence's patent portfolio, which includes more than 233 issued patents worldwide, is a direct result of Rovi's substantial investment in research and development. The asserted MOV Intelligence patents are reflective of this history of innovation, embodying a number of firsts in the development of DRM and watermarking technologies.

39. MOV Intelligence long-term financial success depends in part on its ability to establish, maintain, and protect its proprietary technology through patents. Defendants'

---

[14] Aljean Harmetz, *Cotton Club Cassettes Coded to Foil Pirates*, N.Y. TIMES (April 24, 1985).

[15] *See also* David Nimmer, *Back from the Future: A Proleptic Review of the Digital Millennium Copyright Act*, 16 BERKELEY TECH. L.J. 855, 862 (2001) (The DMCA "contains a welter of corporation-specific features, relating to Macrovision Corp. The features in question relate to section 1201's controls on consumer analog devices.") (citations omitted).

[16] *See* Michael Arnold et al., TECHNIQUES AND APPLICATIONS OF DIGITAL WATERMARKING AND CONTENT PROTECTION 203 (2002) (Describing Rovi's Cactus Data Shield product which by 2002 had been used in over 100 million compact discs. "This scheme [Rovi Cactus Data Shield] operates by inserting illegal data values instead of error-correcting codes."); *see also Rovi SafeDisc Copy Protection Overview*, MACROVISION CORPORATION DATASHEET at 2 (1999) ("SafeDisc incorporates a unique authentication technology that prevents the re-mastering of CD-ROM titles and deters attempts to make unauthorized copies. The SafeDisc authentication process ensures that consumers will only be able to play original discs. The user is forced to purchase a legitimate copy."); Kirby Kish, MACROSAFE SYSTEM: A SOLUTION FOR SECURE DIGITAL MEDIA DISTRIBUTION at 7 (January 2002) (showing the architecture of the MacroSafe system and use of a DRM Server and Key Escrow Server).

infringement presents significant and ongoing damage to MOV Intelligence's business. HPE, Trend Micro and F5 Networks, in an effort to expand their product base and profit from the sale of patented technology, have chosen to incorporate MOV Intelligence's fundamental technology without a license or payment.

THE ASSERTED PATENTS

U.S. PATENT NO. 7,200,230

40. U.S. Patent No. 7,200,230 (the "'230 patent"), entitled "System and Method for Controlling and Enforcing Access Rights to Encrypted Media," was filed January 15, 2001, and claims priority to April 6, 2000. MOV Intelligence is the owner by assignment of the '230 patent. A true and correct copy of the '230 patent is attached hereto as Exhibit A. The '230 patent claims specific methods and systems for extending the capabilities of rights controlled access media systems. Further, the system and methods provide for designation and authentication of the identity of the data processor upon/through which a data object is to be used. The system and methods also provide\ for encryption of a data object and its associated rules such that only a designated data processor can decrypt and use the data object. The system and methods further provide for designation and authentication of the identity of a user by whom the data object is to be used. The system and methods also provide for encryption of a data object and its associated rules such that only a designated user can decrypt and use the data object.

41. The '230 patent has been cited by over 180 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '230 patent as relevant prior art:

- International Business Machines Corporation
- Qualcomm Incorporated
- Autodesk, Inc.
- NTT Docomo, Inc.
- Hitachi, Ltd.
- Koninklijke Phillips Electronics N.C.
- ***Hewlett-Packard Development Company L.P.***

- Time Warner Cable, Inc.
- Cisco Systems, Inc.
- Blackberry Limited
- Arris Enterprises, Inc.
- Meshnetworks, Inc.
- Google, Inc. (now Alphabet, Inc.)
- Oracle Corporation
- General Instrument Corporation
- Symantec Corporation
- Siemens Aktiengesellschaft
- AT&T, Inc.
- Nokia Corporation
- Verizon Communications, Inc.
- Voltage Security, Inc.
- Scientific-Atlanta, Inc. (subsequently acquired by Cisco Systems, Inc.)
- Telefonaktiebolaget LM Ericsson

42. The ‘230 patent claims a technical solution to a problem unique to the transmission of digital information over a network – providing systems and methods for extending the capabilities of rights controlled access to digital content using three layers of encryption.

U.S. PATENT NO. 6,802,006

43. U.S. Patent No. 6,802,006 (the “‘006 patent”), entitled “System and Method of Verifying the Authenticity of Dynamically Connectable Executable Images,” was filed on July 22, 1999, and claims priority to January 15, 1999. MOV Intelligence is the owner by assignment of the ‘006 patent. A true and correct copy of the ‘006 patent is attached hereto as Exhibit B. The ‘006 patent claims specific methods and systems for verifying the authenticity of executable images. The system includes a validator that determines a reference digital signature for an executable image using the contents of the executable image excluding those portions of the executable that are fixed-up by a program loader. The validator then, subsequent to the loading of the executable image, determines an authenticity digital signature to verify that the executable image has not been improperly modified.

44. The ‘006 patent has been cited by over 85 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘006 patent as relevant prior art:

- Intertrust Technologies Corporation
- International Business Machines Corporation
- Intel Corporation
- Microsoft Corporation
- Check Point Software Technologies, Inc.
- Nokia Corporation
- Ipass, Inc.
- Nytell Software LLC
- Amazon Technologies, Inc.
- Panasonic Corporation
- Matsushita Electric Ind. Co. Ltd.
- NXP B.V. (now Cisco Systems, Inc.)
- Intel Corporation
- ***Hewlett-Packard Development Company, L.P.***
- Apple, Inc.
- Lockheed Martin Corporation
- Symantec Corporation
- Zone Labs, Inc.

45. The ‘006 patent claims a technical solution to a problem unique to computer systems: verifying and authenticating executable images.

U.S. PATENT NO. 6,510,516

46. U.S. Patent No. 6,510,516 (the “‘516 patent”), entitled “System and Method for Authenticating Peer Components,” was filed on January 15, 1999, and claims priority to January 16, 1998. MOV Intelligence is the owner by assignment of the ‘516 patent. A true and correct copy of the ‘516 patent is attached hereto as Exhibit C. The ‘516 patent claims specific methods and systems for controlling the usage of data objects in component object systems. According to the invention, each data object includes a peer list that defines one or more peer data objects that are required by the data object. Upon receipt of a data object, the system verifies the integrity of the data object. Further, the system identifies the integrity of the peer data objects.

47. The ‘516 patent family has been cited by over 108 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘516 patent as relevant prior art:

- America Online, Inc.
- LG Electronics, Inc.
- Microsoft Corporation
- Samsung Electronics Co., Ltd.
- First Data Corporation
- International Business Machines Corporation
- Pixar, Inc. (now a subsidiary of the Walt Disney Company)
- Adobe Systems Incorporated
- The Western Union Company
- Verizon Communications, Inc.
- JPMorgan Chase & Co.
- Electronics and Telecommunications Research Institute (ETRI)
- Siemens Medical Solutions USA, Inc.

U.S. PATENT NO. 7,650,504

48. U.S. Patent No. 7,650,504 (the “‘504 patent”), entitled “System and Method of Verifying the Authenticity of Dynamically Connectable Executable Images,” was filed on August 23, 2004, and claims priority to July 22, 1999. MOV Intelligence is the owner by assignment of the ‘504 patent. A true and correct copy of the ‘504 patent is attached hereto as Exhibit D. The ‘504 patent claims specific methods and systems for verifying the authenticity of executable images. The systems and methods taught in the ‘504 patent incorporate a validator that determines a reference digital signature for an executable image using the contents of the executable image excluding those portions of the executable that are fixed-up by a program loader. The validator then, subsequent to the loading of the executable image, determines an authenticity digital signature to verify that the executable image has not been improperly modified. In addition, the validator ensures that each of the pointers in the executable image have not been improperly redirected.

49. The ‘504 patent and its underlying application have been cited by over 30 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘504 patent as relevant prior art:

- Qualcomm Incorporated
- Intel Corporation
- Micro Beef Technologies, Ltd
- Microsoft Corporation
- Apple, Inc.
- Symantec Corporation
- Samsung Electronics Co., Ltd.
- Cybersoft Technologies, Inc.
- Electronics and Telecommunications Research Institute (ETRI)

50. The ‘504 patent claims a technical solution to a problem unique to the transmission of digital information over a network: verifying the identity of a software application in a dynamic loading environment. In particular, the system determines whether a software application that has been dynamically connected to another data object has been tampered with subsequent to the execution of the software application.

U.S. PATENT NO. 7,650,418

51. U.S. Patent No. 7,650,418 (the “‘418 patent”), entitled “System and Method for Controlling the Usage of Digital Objects,” was filed on August 26, 2004, and claims priority to December 8, 1998. MOV Intelligence is the owner by assignment of the ‘418 patent. A true and correct copy of the ‘418 patent is attached hereto as Exhibit E. The ‘418 patent claims specific methods and systems for controlling the usage of digital objects wherein control rights associated with a digital data object activate an external control object and an intercept application to intercept and monitor communications between a hosting application and a document server application associated with the creation of the digital data object. The ‘418 patent teaches the use of intercepting and monitoring functions without affecting or changing the hosting application or the document server application. The external control object activates an intercept application which mimics the functions of the document server application and performs user actions on the digital data object as authorized by the external control object according to the

control rights associated with the digital object. By intercepting and monitoring user actions on a digital data object, the invention can control access and use of the digital data object.

52. The ‘418 patent family has been cited by over 47 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘418 patent as relevant prior art:

- Google, Inc.
- Fisher-Rosemount Systems, Inc.
- Knoa Software, Inc.
- Securewave S.A.
- International Business Machines Corporation
- Ab Initio Technology LLC
- The Invention Science Fund I, LLC
- Searete LLC
- Microsoft Corporation

53. The ‘418 patent claims a technical solution to a problem unique to the transmission of digital information over a network: reliably controlling the usage of digital objects wherein the system and/or methods intercept the communication between two applications communicating over a computer network.

U.S. PATENT NO. 7,124,114

54. U.S. Patent No. 7,124,114 (the “‘114 patent”), entitled “Method and Apparatus for Determining Digital A/V Content Distribution Terms Based on Detected Piracy Levels,” was filed on November 9, 2000. MOV Intelligence is the owner by assignment of the ‘114 patent. A true and correct copy of the ‘114 patent is attached hereto as Exhibit F. The ‘114 patent claims specific methods and systems for distributing copyrighted material over a computer network. Specifically, the ‘114 patent teaches the providing of protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to the prospective recipient; and providing or withholding a copy of the protected material to the prospective recipient in accordance with the terms. The ‘114 patent also discloses the use of a first set of program code which serves to ascertain terms for providing a protected material to a prospective recipient according at least in part to information of

unauthorized copying of other protected material previously provided to the prospective recipient. The first set of program code also serves to provide or withhold a copy of the protected material to or from the prospective recipient in accordance with the terms.

55. The '114 patent family has been cited by over 39 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '114 patent as relevant prior art:

- Google, Inc.
- NBCUniversal Media, Inc.
- Digimarc Corporation
- ***Hewlett-Packard Development Company, L.P.***
- Aigo Research Institute of Image Computing Co., Ltd.
- AT&T Intellectual Property I, L.P.
- General Electric Company
- The Nielsen Company (US), LLC
- Sca Ipla Holdings, Inc.
- Thomson Licensing, Inc.
- Fujitsu Limited

56. The '114 patent claims a technical solution to a problem unique to the transmission of digital information over a network: preventing the unauthorized copying of digital content. The patent teaches the use of a server that manages access to content according to terms determined from information stored in a database of prior unauthorized copying attributed to that recipient.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 7,200,230

57. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

58. HPE designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for digital rights management.

59. HPE designs, makes, sells, offers to sell, imports, and/or uses the HPE Atalla Secure Configuration Assistant-3 product (the "HPE '230 Product(s)").

60. On information and belief, one or more HPE subsidiaries and/or affiliates use the HPE '230 Products in regular business operations.

61. On information and belief, one or more of the HPE '230 Products include digital rights management technology.

62. On information and belief, one or more of the HPE '230 Products enable associating a user program key with a user program configured to run on a user data processor.

63. On information and belief, the HPE '230 Products are available to businesses and individuals throughout the United States.

64. On information and belief, the HPE '230 Products are provided to businesses and individuals located in the Eastern District of Texas.

65. On information and belief, the HPE '230 Products enable determining whether the use of the data object is to be restricted to a particular user data processor.

66. On information and belief, the HPE '230 Products comprise a system wherein a machine key device is associated with the particular user data processor. Further, the machine key device is accessible by the user program, and the machine key device maintains a portion of a machine key.

67. On information and belief, the HPE '230 Products enable encrypting a data object so the decryption of a first secure layer and a second secure layer of the encrypted data object requires the user program key and the machine key.

68. On information and belief, the HPE '230 Products enable determining whether the use of the data object is to be restricted to a particular user.

69. On information and belief, the HPE '230 Products provide for the designation and authentication of the identity of a user by whom the data object is to be used.

70. On information and belief, the HPE '230 Products enable associating a user key device with the particular user. Further, the HPE '230 Products enable the user key device to be made accessible by the user program. And, the user key device maintains a portion of a user key.

71. On information and belief, the HPE '230 Products contain functionality for encrypting a data object so the decryption of a third secure layer of the encrypted data object requires the user key.

72. On information and belief, the HPE '230 Products contain functionality wherein the third key used by the system for managing digital rights is the media access controller (MAC) address of the user data processor.

73. On information and belief, the HPE '230 Products provide for encryption of a data object so only a designated data processor can decrypt and use the data object.

74. On information and belief, the HPE '230 Products enable user specific digital rights management authorization and access.

75. On information and belief, HPE has directly infringed and continues to directly infringe the '230 patent by, among other things, making, using, offering for sale, and/or selling digital content protection technology, including but not limited to the HPE '230 Products, which include infringing digital rights management technology. Such products and/or services include, by way of example and without limitation, the HPE Atalla Secure Configuration Assistant-3.

76. By making, using, testing, offering for sale, and/or selling digital rights management products and services, including but not limited to the HPE '230 Products, HPE has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '230 patent, including at least claim 39, pursuant to 35 U.S.C. § 271(a).

77. On information and belief, HPE also indirectly infringes the '230 patent by actively inducing infringement under 35 USC § 271(b).

78. On information and belief, HPE had knowledge of the '230 patent since at least July 7, 2009 based on HPE's citation of the '230 patent in the prosecution of patents that were assigned to HPE subsidiaries and/or affiliates. Specifically, the following patents assigned to HPE reference the '230 patent as relevant prior art: U.S. Patent No. 7,961,879 (citing the '230 patent and assigned to HPE subsidiary Voltage Security, Inc.); U.S. Patent No. 7,580,521 (citing the '230 patent and assigned to HPE subsidiary Voltage Security, Inc.); and U.S. Patent No.

7,558,954 (citing the ‘230 patent and assigned to Hewlett-Packard Development Company, L.P.).

79. In the alternative, HPE has had knowledge of the ‘230 patent since at least the service of this Complaint or shortly thereafter, and on information and belief, HPE knew of the ‘230 patent and knew of its infringement, including by way of this lawsuit.

80. On information and belief, HPE intended to induce patent infringement by third-party customers and users of the HPE ‘230 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. HPE specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘230 patent. HPE performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘230 patent and with the knowledge that the induced acts would constitute infringement. For example, HPE provides the HPE ‘230 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘230 patent, including at least claim 39, and HPE further provides documentation and training materials that cause customers and end users of the HPE ‘230 Products to utilize the products in a manner that directly infringe one or more claims of the ‘230 patent. By providing instruction and training to customers and end-users on how to use the HPE ‘230 Products in a manner that directly infringes one or more claims of the ‘230 patent, including at least claim 39, HPE specifically intended to induce infringement of the ‘230 patent. On information and belief, HPE engaged in such inducement to promote the sales of the HPE ‘230 Products, e.g., through HPE user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘230 patent. Accordingly, HPE has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘230 patent, knowing that such use constitutes infringement of the ‘230 patent.

81. The ‘230 patent is well-known within the industry as demonstrated by the over 180 citations to the ‘230 patent family in published patents and published patent applications

assigned to technology companies and academic institutions. Several of HPE's competitors have paid considerable licensing fees for their use of the technology claimed by the '230 patent. In an effort to gain an advantage over HPE's competitors by utilizing the same licensed technology without paying reasonable royalties, HPE infringed the '230 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

82. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '230 patent.

83. As a result of HPE's infringement of the '230 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for HPE's infringement, but in no event less than a reasonable royalty for the use made of the invention by HPE together with interest and costs as fixed by the Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 6,802,006

84. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

85. HPE designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for determining the authenticity of an executable image.

86. HPE designs, makes, sells, offers to sell, imports, and/or uses the HPE iLO 4 and HPE iLO 3 Products (the "HPE '006 Product(s)").

87. On information and belief, one or more HPE subsidiaries and/or affiliates use the HPE '006 Products in regular business operations.

88. On information and belief, one or more of the HPE '006 Products include authentication technology.

89. On information and belief, one or more of the HPE '006 Products enable authenticating the identity of a software application in a dynamic loading environment. In

particular, the HPE ‘006 Products determine whether an executable image has been dynamically connected to another data object that has been tampered with subsequent to the execution of the software application.

90. On information and belief, the HPE ‘006 Products are available to businesses and individuals throughout the United States.

91. On information and belief, the HPE ‘006 Products are provided to businesses and individuals located in the Eastern District of Texas.

92. On information and belief, the HPE ‘006 Products enable identifying one or more locations within the executable image, each of the identified locations being modified by a program loader.

93. On information and belief, the HPE ‘006 Products comprise a system wherein a reference digital signature is generated based on an executable image.

94. On information and belief, the HPE ‘006 Products generate a reference digital signature that excludes one or more locations in an executable image.

95. On information and belief, the HPE ‘006 Products are capable of storing the reference digital signature on a computer network.

96. On information and belief, the HPE ‘006 Products comprise systems and methods wherein an authenticity digital signature is generated based on an executable image.

97. On information and belief, the HPE ‘006 Products comprise systems and methods that generate an authenticity digital signature that excludes one or more locations in an executable image.

98. On information and belief, the HPE ‘006 Products comprise systems and methods that determine whether the authenticity digital signature matches the reference digital signature.

99. On information and belief, the HPE ‘006 Products contain functionality that generates a warning if the reference digital signature does not match the authenticity digital signature.

100. On information and belief, the HPE ‘006 Products contain functionality wherein the digital signature is generated based on a first and second point in time. For example, one or more of the HPE ‘006 Products generate a reference digital signature at a first point in time. Subsequently, an authenticity digital signature is generated (at a second point in time).

101. On information and belief, the HPE ‘006 Products comprise a system and method that generates a digital signature based on a hash value. Specifically, the reference digital signature that is generated by the HPE ‘006 Products at a first point in time is based on a hash value. Later the authenticity digital signature is also generated based on a hash function that is used to check data integrity.

102. On information and belief, the HPE ‘006 Products comprise a system and method that can verify the identity a computer application.

103. On information and belief, the HPE ‘006 Products enable the detection of corrupted data in a computer image.

104. On information and belief, the HPE ‘006 Products enable the verification of the integrity of software images.

105. On information and belief, HPE has directly infringed and continues to directly infringe the ‘006 patent by, among other things, making, using, offering for sale, and/or selling content protection technology, including but not limited to the HPE ‘006 Products, which includes technology for verifying the authenticity of a software image. Such products and/or services include, by way of example and without limitation, the HPE iLO 4 and HPE iLO 3 Products.

106. By making, using, testing, offering for sale, and/or selling verification and authentication products and services, including but not limited to the HPE ‘006 Products, HPE has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the ‘006 patent, including at least claims 1, 3, 14, and 15, pursuant to 35 U.S.C. § 271(a).

107. On information and belief, HPE also indirectly infringes the ‘006 patent by actively inducing infringement under 35 USC § 271(b).

108. On information and belief, HPE had knowledge of the ‘006 patent since at least November 1, 2011, based on published patents and patent applications assigned to HPE subsidiaries and/or affiliates referencing the ‘006 patent at relevant prior art. Specifically, the following patents and published patent applications assigned to HPE reference the ‘006 patent as relevant prior art: U.S. Patent App. No. 2007/0220500 (citing the ‘006 patent and assigned to Hewlett-Packard Development Company, L.P.) and U.S. Patent No. 8,051,299 (citing the ‘006 patent and assigned to Hewlett-Packard Development Company, L.P.)

109. In the alternative, HPE has had knowledge of the ‘006 patent since at least the service of this Complaint or shortly thereafter, and on information and belief, HPE knew of the ‘006 patent and knew of its infringement, including by way of this lawsuit.

110. On information and belief, HPE intended to induce patent infringement by third-party customers and users of the HPE ‘006 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. HPE specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘006 patent. HPE performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘006 patent and with the knowledge that the induced acts would constitute infringement. For example, HPE provides the HPE ‘006 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘006 patent, including at least claims 1, 3, 14, and 15, and HPE further provides documentation and training materials that cause customers and end users of the HPE ‘006 Products to utilize the products in a manner that directly infringe one or more claims of the ‘006 patent. By providing instruction and training to customers and end-users on how to use the HPE ‘006 Products in a manner that directly infringes one or more claims of the ‘006 patent, including at least claims 1, 3, 14, and 15, HPE specifically intended to induce infringement of the ‘006 patent. On information and belief, HPE engaged in such inducement to

promote the sales of the HPE '006 Products, *e.g.*, through HPE user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '006 patent. Accordingly, HPE has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '006 patent, knowing that such use constitutes infringement of the '006 patent.

111. The '006 patent is well-known within the industry as demonstrated by the over 85 citations to the '006 patent in issued patents and published patent applications assigned to technology companies and academic institutions. Several of HPE's competitors have paid considerable licensing fees for their use of the technology claimed by the '006 patent. In an effort to gain an advantage over HPE's competitors by utilizing the same licensed technology without paying reasonable royalties, HPE infringed the '006 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

112. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '006 patent.

113. As a result of HPE's infringement of the '006 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for HPE's infringement, but in no event less than a reasonable royalty for the use made of the invention by HPE together with interest and costs as fixed by the Court.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 6,510,516

114. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

115. HPE designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for authenticating peer data objects.

116. HPE designs, makes, sells, offers to sell, imports, and/or uses the HPE WebRTC Gateway controller; HPE Multimedia Services Environment (MSE); and WebRTC Gateway Controller (the "HPE '516 Product(s)").

117. On information and belief, one or more HPE subsidiaries and/or affiliates use the HPE '516 Products in regular business operations.

118. On information and belief, one or more of the HPE '516 Products include authentication technology.

119. On information and belief, one or more of the HPE '516 Products enable authenticating the identity of peers to a data object.

120. On information and belief, the HPE '516 Products are available to businesses and individuals throughout the United States.

121. On information and belief, the HPE '516 Products are provided to businesses and individuals located in the Eastern District of Texas.

122. On information and belief, the HPE '516 Products enable first data objects to contain or be linked to a description of one or more peer data objects that are required to be connected to the first data object before the data object can be accessed by the peer data objects.

123. On information and belief, the HPE '516 Products enable the use of a digital signature that identifies the provider of a data object.

124. On information and belief, the HPE '516 Products contain systems and methods that comprise reading from a data object a description of one or more peer data objects that is required for use of the data object.

125. On information and belief, the HPE '516 Products contain functionality for determining whether the data object is authorized to communicate with one or more peer data objects.

126. On information and belief, the HPE '516 Products contain the capability to determine if the data object is authorized to communicate with one or more peer data objects.

127. On information and belief, the HPE ‘516 Products are capable of controlling the connection of the peer data objects to the data object.

128. On information and belief, the HPE ‘516 Products comprise systems and methods that connect a data object to peer data objects based upon authorization being granted. Moreover, when authorization is granted for the connection of a data object to peer data objects the peer data objects can communicate with the data object and the data object can communicate with the peer data objects.

129. On information and belief, the HPE ‘516 Products support authenticating a data object where the data object is encrypted.

130. On information and belief, HPE has directly infringed and continues to directly infringe the ‘516 patent by, among other things, making, using, offering for sale, and/or selling data object authentication and verification technology, including but not limited to the HPE ‘516 Products, which include infringing verification and authentication technologies. Such products and/or services include, by way of example and without limitation, the HPE WebRTC Gateway controller; HPE Multimedia Services Environment (MSE); and WebRTC Gateway Controller.

131. By making, using, testing, offering for sale, and/or selling authentication and verification products and services, including but not limited to the HPE ‘516 Products, HPE has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the ‘516 patent, including at least claims 1, 17, and 20, pursuant to 35 U.S.C. § 271(a).

132. On information and belief, HPE also indirectly infringes the ‘516 patent by actively inducing infringement under 35 USC § 271(b).

133. On information and belief, HPE had knowledge of the ‘516 patent since at least service of this Complaint or shortly thereafter, and on information and belief, HPE knew of the ‘516 patent and knew of its infringement, including by way of this lawsuit.

134. On information and belief, HPE intended to induce patent infringement by third-party customers and users of the HPE ‘516 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would

cause infringement. HPE specifically intended and was aware that the normal and customary use of the accused products would infringe the '516 patent. HPE performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '516 patent and with the knowledge that the induced acts would constitute infringement. For example, HPE provides the HPE '516 Products that have the capability of operating in a manner that infringe one or more of the claims of the '516 patent, including at least claims 1, 17, and 20, and HPE further provides documentation and training materials that cause customers and end users of the HPE '516 Products to utilize the products in a manner that directly infringe one or more claims of the '516 patent. By providing instruction and training to customers and end-users on how to use the HPE '516 Products in a manner that directly infringes one or more claims of the '516 patent, including at least claims 1, 17, and 20, HPE specifically intended to induce infringement of the '516 patent. On information and belief, HPE engaged in such inducement to promote the sales of the HPE '516 Products, e.g., through HPE user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '516 patent. Accordingly, HPE has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '516 patent, knowing that such use constitutes infringement of the '516 patent.

135. The '516 patent is well-known within the industry as demonstrated by the over 108 citations to the '516 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, LG Electronics, Inc. and Siemens AG). Several of HPE's competitors have paid considerable licensing fees for their use of the technology claimed by the '516 patent. In an effort to gain an advantage over HPE's competitors by utilizing the same licensed technology without paying reasonable royalties, HPE infringed the '516 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

136. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '516 patent.

137. As a result of HPE's infringement of the '516 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for HPE's infringement, but in no event less than a reasonable royalty for the use made of the invention by HPE together with interest and costs as fixed by the Court.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 7,650,504

138. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

139. HPE designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for verifying the authenticity of executable images.

140. HPE designs, makes, sells, offers to sell, imports, and/or uses the HP Service Manager Version 9.34, HP Service Manager Version 9.4, and HP Service Manager Version 9.41 (the "HPE '504 Product(s)").

141. On information and belief, one or more HPE subsidiaries and/or affiliates use the HPE '504 Products in regular business operations.

142. On information and belief, one or more of the HPE '504 Products include authentication technology.

143. On information and belief, one or more of the HPE '504 Products comprise systems and methods for determining the authenticity of an executable image.

144. On information and belief, one or more of the HPE '504 Products enable authenticating and verifying an executable image. In particular, the HPE '504 Products determine whether a software application that has been dynamically connected to another data object has been tampered with subsequent to the execution of the software application.

145. On information and belief, the HPE '504 Products are available to businesses and individuals throughout the United States.

146. On information and belief, the HPE ‘504 Products are provided to businesses and individuals located in the Eastern District of Texas.

147. On information and belief, the HPE ‘504 Products enable the use of a reference digital signature for an executable image. The reference digital signature uses the contents of the executable image excluding portions of the executable that are fixed-up by a program loader.

148. On information and belief, the HPE ‘504 Products comprise a system wherein a reference digital signature is generated based on an executable image.

149. On information and belief, the HPE ‘504 Products generate a reference digital signature that excludes one or more locations in an executable image.

150. On information and belief, the HPE ‘504 Products comprise systems and methods wherein subsequent to the loading of the executable image the ‘504 Products determine an authenticity digital signature to verify that the executable image has not been improperly modified.

151. On information and belief, the HPE ‘504 Products comprise systems and methods that generate an authenticity digital signature that excludes one or more locations in an executable image.

152. On information and belief, the HPE ‘504 Products are systems and methods that generate an authenticity digital signature after the executable image is loaded into memory. The authenticity digital signature which is generated by the HPE ‘504 Products excludes one or more pointers in need of fixing up;

153. On information and belief, the HPE ‘504 Products comprise systems and methods that determine whether the authenticity digital signature matches the reference digital signature.

154. On information and belief, the HPE ‘504 Products enable the generating of a reference digital signature prior to loading the executable image into memory. Specifically, the HPE ‘504 Products generate a reference digital signature that excludes one or more pointers from the reference digital signature.

155. On information and belief, the HPE '504 Products contain functionality wherein the digital signature is generated based on a first and second point in time.

156. On information and belief, the HPE '504 Products have the ability to compare the reference digital signature and the authenticity digital signature to perform an authenticity check.

157. On information and belief, the HPE '504 Products enable the detection of corrupted data in a computer image.

158. On information and belief, the HPE '504 Products enable the verification of the integrity of software images.

159. On information and belief, HPE has directly infringed and continues to directly infringe the '504 patent by, among other things, making, using, offering for sale, and/or selling content protection technology, including but not limited to the HPE '504 Products, which includes technology for verifying the authenticity of a software image. Such products and/or services include, by way of example and without limitation, the HP Service Manager Version 9.34, HP Service Manager Version 9.4, and HP Service Manager Version 9.41.

160. By making, using, testing, offering for sale, and/or selling authentication and verification technologies and services, including but not limited to the HPE '504 Products, HPE has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '504 patent, including at least claims 1 and 10, pursuant to 35 U.S.C. § 271(a).

161. On information and belief, HPE also indirectly infringes the '504 patent by actively inducing infringement under 35 USC § 271(b).

162. On information and belief, HPE had knowledge of the '504 patent since at least service of this Complaint or shortly thereafter, and on information and belief, HPE knew of the '504 patent and knew of its infringement, including by way of this lawsuit.

163. On information and belief, HPE intended to induce patent infringement by third-party customers and users of the HPE '504 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would

cause infringement. HPE specifically intended and was aware that the normal and customary use of the accused products would infringe the '504 patent. HPE performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '504 patent and with the knowledge that the induced acts would constitute infringement. For example, HPE provides the HPE '504 Products that have the capability of operating in a manner that infringe one or more of the claims of the '504 patent, including at least claims 1 and 10, and HPE further provides documentation and training materials that cause customers and end users of the HPE '504 Products to utilize the products in a manner that directly infringe one or more claims of the '504 patent. By providing instruction and training to customers and end-users on how to use the HPE '504 Products in a manner that directly infringes one or more claims of the '504 patent, including at least claims 1 and 10, HPE specifically intended to induce infringement of the '504 patent. On information and belief, HPE engaged in such inducement to promote the sales of the HPE '504 Products, e.g., through HPE user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '504 patent. Accordingly, HPE has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '504 patent, knowing that such use constitutes infringement of the '504 patent.

164. The '504 patent is well-known within the industry as demonstrated by the over 30 citations to the '504 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Apple, Inc. and Electronics and Telecommunications Research Institute (ETRI)). Several of HPE's competitors have paid considerable licensing fees for their use of the technology claimed by the '504 patent. In an effort to gain an advantage over HPE's competitors by utilizing the same licensed technology without paying reasonable royalties, HPE infringed the '504 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

165. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘504 patent.

166. As a result of HPE’s infringement of the '504 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for HPE’s infringement, but in no event less than a reasonable royalty for the use made of the invention by HPE together with interest and costs as fixed by the Court.

COUNT V
INFRINGEMENT OF U.S. PATENT NO. 7,650,418

167. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

168. HPE and F5 Networks designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for controlling the usage of digital objects.

169. HPE and F5 Networks, in a joint enterprise, designs, makes, sells, offers to sell, imports, and/or uses a joint solution, the HPE Atalla HSM and F5-BIG IP Local Traffic Manager Solution (“HPE-HSM F5-LTM Product” or “HPE-F5 Networks ‘418 Product(s)”).

170. On information and belief, one or more HPE and F5 Networks subsidiaries and/or affiliates use the HPE-F5 Networks ‘418 Products in regular business operations.

171. On information and belief, one or more of the HPE-F5 Networks ‘418 Products comprise systems and methods for intercepting a communication between two applications in a computer environment.

172. On information and belief, one or more of the HPE-F5 Networks ‘418 Products enable intercepting a communication between two applications where the first and second application communicate via a predefined communications channel.

173. On information and belief, the HPE-F5 Networks ‘418 Products are available to businesses and individuals throughout the United States.

174. On information and belief, the HPE-F5 Networks '418 Products are provided to businesses and individuals located in the Eastern District of Texas.

175. On information and belief, the HPE-F5 Networks '418 Products include systems and methods that comprise a discreet intercept technology component (DIT) and a dynamic connection logic component (DCL).

176. On information and belief, the HPE-F5 Networks '418 Products comprise systems and methods wherein the DIT component permits the interception of communication and data flows between two or more components in component-based applications.

177. On information and belief, the HPE-F5 Networks '418 Products enable the DIT component to be inserted between two digital components. The DIT then intercepts the data and communications, thereby controlling the communication between the two digital components.

178. On information and belief, the HPE-F5 Networks '418 Products comprise systems and methods that enable a control object capable of specifying a dynamic control logic depending on the intercepted data communication.

179. On information and belief, the HPE-F5 Networks '418 Products enable applying by the intercept application the dynamic control logic specified by the control object on the digital object.

180. On information and belief, the HPE-F5 Networks '418 Products contain functionality for intercepting data communication between a first application and a second application within a computer network without changing the functionality of the first application and the second application.

181. On information and belief, HP and F5 Networks have directly infringed and continue to directly infringe the '418 patent by, among other things, making, using, offering for sale, and/or selling digital rights technology, including but not limited to the HPE-F5 Networks '418 Products, which include infringing technology for controlling the usage of data objects. Such products and/or services include, by way of example and without limitation, the HPE Atalla HSM and F5-BIG IP Local Traffic Manager Solution.

182. By making, using, testing, offering for sale, and/or selling digital rights management products and services, including but not limited to the HPE-F5 Networks '418 Products, HPE and F5 Networks have injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '418 patent, including at least claims 1, 2, 4, 7, 8, and 9, pursuant to 35 U.S.C. § 271(a).

183. On information and belief, HPE and F5 Networks also indirectly infringes the '418 patent by actively inducing infringement under 35 USC § 271(b).

184. On information and belief, HPE and F5 Networks had knowledge of the '418 patent since at least service of this Complaint or shortly thereafter, and on information and belief, HPE and F5 Networks knew of the '418 patent and knew of its infringement, including by way of this lawsuit.

185. On information and belief, HPE and F5 Networks intended to induce patent infringement by third-party customers and users of the HPE-F5 Networks '418 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. HPE and F5 Networks specifically intended and were aware that the normal and customary use of the accused products would infringe the '418 patent. HPE and F5 Networks performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '418 patent and with the knowledge that the induced acts would constitute infringement. For example, HPE and F5 Networks provide the HPE-F5 Networks '418 Products that have the capability of operating in a manner that infringe one or more of the claims of the '418 patent, including at least claims 1, 2, 4, 7, 8, and 9, and HPE and F5 Networks further provide documentation and training materials that cause customers and end users of the HPE-F5 Networks '418 Products to utilize the products in a manner that directly infringe one or more claims of the '418 patent. By providing instruction and training to customers and end-users on how to use the HPE-F5 Networks '418 Products in a manner that directly infringes one or more claims of the '418 patent, including at least claims 1, 2, 4, 7, 8, and 9, HPE and F5 Networks specifically intended to induce

infringement of the ‘418 patent. On information and belief, HPE and F5 Networks engaged in such inducement to promote the sales of the HPE-F5 Networks ‘418 Products, e.g., through HPE and F5 Networks user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘418 patent. Accordingly, HPE and F5 Networks have induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘418 patent, knowing that such use constitutes infringement of the ‘418 patent.

186. The ‘418 patent is well-known within the industry as demonstrated by the over 47 citations to the ‘418 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Google, Inc. and International Business Machines Corporation). Several of HPE and F5 Networks’ competitors have paid considerable licensing fees for their use of the technology claimed by the ‘418 patent. In an effort to gain an advantage over HPE and F5 Networks’ competitors by utilizing the same licensed technology without paying reasonable royalties, HPE and F5 Networks infringed the ‘418 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

187. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘418 patent.

188. As a result of HPE and F5 Networks’ infringement of the '418 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for HPE and F5 Networks’ infringement, but in no event less than a reasonable royalty for the use made of the invention by HPE and F5 Networks together with interest and costs as fixed by the Court.

COUNT VI
HPE'S INFRINGEMENT OF U.S. PATENT NO. 7,124,114

189. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

190. HPE designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for managing the distribution of digital content and preventing unauthorized access to protected digital content.

191. HPE designs, makes, sells, offers to sell, imports, and/or uses the HP Security Management System H3 Appliance, HP Security Management System H3 XL Appliance, and HP vSMS Essential for VMware virtual appliance (the "HPE '114 Product(s)").

192. On information and belief, one or more HPE subsidiaries and/or affiliates use the HPE '114 Products in regular business operations.

193. On information and belief, one or more of the HPE '114 Products include content protection and content access technology.

194. On information and belief, one or more of the HPE '114 Products enable providing or withholding access to digital content is accordance with digital rights management protection terms.

195. On information and belief, the HPE '114 Products are available to businesses and individuals throughout the United States.

196. On information and belief, the HPE '114 Products are provided to businesses and individuals located in the Eastern District of Texas.

197. On information and belief, the HPE '114 Products enable the distribution of protected digital data.

198. On information and belief, the HPE '114 Products comprise systems and methods wherein the HPE '114 Products ascertain terms for providing protected data to a prospective requestor according at least in part to information of unauthorized copying of other protected material previously provided to said prospective requestor.

199. On information and belief, the HPE '114 Products comprise systems and methods that provide authorization to allow access or deny access to protected digital data based on ascertained terms.

200. On information and belief, HPE has directly infringed and continues to directly infringe the '114 patent by, among other things, making, using, offering for sale, and/or selling digital content protection technology, including but not limited to the HPE '114 Products, which include infringing digital rights management technologies. Such products and/or services include, by way of example and without limitation, the HP Security Management System H3 Appliance, HP Security Management System H3 XL Appliance, and HP vSMS Essential for VMware virtual appliance.

201. By making, using, testing, offering for sale, and/or selling digital rights management and access control products and services, including but not limited to the HPE '114 Products, HPE has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '114 patent, including at least claims 1, 21, 41, and 52, pursuant to 35 U.S.C. § 271(a).

202. On information and belief, HPE also indirectly infringes the '114 patent by actively inducing infringement under 35 USC § 271(b).

203. On information and belief, HPE had knowledge of the '114 patent since at least August 19, 2008, based on HPE's citation of the '114 patent in the prosecution of patents that were assigned to HPE subsidiaries and/or affiliates. Specifically, the following patents and published patent applications assigned to HPE reference the '114 patent as relevant prior art: U.S. Patent App. No. 2004/0086125 (citing the '114 patent and assigned to Hewlett-Packard Development Company, L.P.) and U.S. Patent No. 7,415,113 (citing the '114 patent and assigned to Hewlett-Packard Development Company, L.P.).

204. In the alternative, HPE has had knowledge of the '114 patent since at least service of this Complaint or shortly thereafter, and on information and belief, HPE knew of the '114 patent and knew of its infringement, including by way of this lawsuit.

205. On information and belief, HPE intended to induce patent infringement by third-party customers and users of the HPE '114 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. HPE specifically intended and was aware that the normal and customary use of the accused products would infringe the '114 patent. HPE performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '114 patent and with the knowledge that the induced acts would constitute infringement. For example, HPE provides the HPE '114 Products that have the capability of operating in a manner that infringe one or more of the claims of the '114 patent, including at least claims 1, 21, 41, and 52, and HPE further provides documentation and training materials that cause customers and end users of the HPE '114 Products to utilize the products in a manner that directly infringe one or more claims of the '114 patent. By providing instruction and training to customers and end-users on how to use the HPE '114 Products in a manner that directly infringes one or more claims of the '114 patent, including at least claims 1, 21, 41, and 52, HPE specifically intended to induce infringement of the '114 patent. On information and belief, HPE engaged in such inducement to promote the sales of the HPE '114 Products, e.g., through HPE user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '114 patent. Accordingly, HPE has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '114 patent, knowing that such use constitutes infringement of the '114 patent.

206. The '114 patent is well-known within the industry as demonstrated by the over 39 citations to the '114 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Aigo Research Institute of Image Computing Co., Ltd. and General Electric Company). Several of HPE's competitors have paid considerable licensing fees for their use of the technology claimed by the '114 patent. In an effort to gain an advantage over HPE's competitors by utilizing the same licensed technology without paying reasonable royalties, HPE infringed the '114 patent in a manner best described as

willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

207. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘114 patent.

208. As a result of HPE’s infringement of the '114 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for HPE’s infringement, but in no event less than a reasonable royalty for the use made of the invention by HPE together with interest and costs as fixed by the Court.

COUNT VII
TREND MICRO’S INFRINGEMENT OF U.S. PATENT NO. 7,124,114

209. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

210. Trend Micro designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for managing the distribution of digital content and preventing unauthorized access to protected digital content.

211. Trend Micro designs, makes, sells, offers to sell, imports, and/or uses the Trend Micro TippingPoint Security Management System H3 Appliance, Trend Micro TippingPoint Security Management System H3 XL Appliance, Trend Micro TippingPoint vSMS Essential Virtual Appliance, and Trend Micro TippingPoint vSMS Enterprise Virtual Appliance (the “Trend Micro ‘114 Product(s)”).

212. On information and belief, one or more Trend Micro subsidiaries and/or affiliates use the Trend Micro ‘114 Products in regular business operations.

213. On information and belief, one or more of the Trend Micro ‘114 Products include content protection and content access technology.

214. On information and belief, one or more of the Trend Micro '114 Products enable providing or withholding access to digital content is accordance with digital rights management protection terms.

215. On information and belief, the Trend Micro '114 Products are available to businesses and individuals throughout the United States.

216. On information and belief, the Trend Micro '114 Products are provided to businesses and individuals located in the Eastern District of Texas.

217. On information and belief, the Trend Micro '114 Products enable the distribution of protected digital data.

218. On information and belief, the Trend Micro '114 Products comprise systems and methods wherein the Trend Micro '114 Products ascertain terms for providing protected data to a prospective requestor according at least in part to information of unauthorized copying of other protected material previously provided to said prospective requestor.

219. On information and belief, the Trend Micro '114 Products comprise systems and methods that provide authorization to allow access or deny access to protected digital data based on ascertained terms.

220. On information and belief, Trend Micro has directly infringed and continues to directly infringe the '114 patent by, among other things, making, using, offering for sale, and/or selling digital content protection technology, including but not limited to the Trend Micro '114 Products, which include infringing digital rights management technologies. Such products and/or services include, by way of example and without limitation, the Trend Micro TippingPoint Security Management System H3 Appliance, Trend Micro TippingPoint Security Management System H3 XL Appliance, Trend Micro TippingPoint vSMS Essential Virtual Appliance, and Trend Micro TippingPoint vSMS Enterprise Virtual Appliance.

221. By making, using, testing, offering for sale, and/or selling digital rights management and access control products and services, including but not limited to the Trend Micro '114 Products, Trend Micro has injured MOV Intelligence and is liable to MOV

Intelligence for directly infringing one or more claims of the ‘114 patent, including at least claims 1, 21, 41, and 52, pursuant to 35 U.S.C. § 271(a).

222. On information and belief, Trend Micro also indirectly infringes the ‘114 patent by actively inducing infringement under 35 USC § 271(b).

223. On information and belief, Trend Micro had knowledge of the ‘114 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Trend Micro knew of the ‘114 patent and knew of its infringement, including by way of this lawsuit.

224. On information and belief, Trend Micro intended to induce patent infringement by third-party customers and users of the Trend Micro ‘114 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Trend Micro specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘114 patent. Trend Micro performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘114 patent and with the knowledge that the induced acts would constitute infringement. For example, Trend Micro provides the Trend Micro ‘114 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘114 patent, including at least claims 1, 21, 41, and 52, and Trend Micro further provides documentation and training materials that cause customers and end users of the Trend Micro ‘114 Products to utilize the products in a manner that directly infringe one or more claims of the ‘114 patent. By providing instruction and training to customers and end-users on how to use the Trend Micro ‘114 Products in a manner that directly infringes one or more claims of the ‘114 patent, including at least claims 1, 21, 41, and 52, Trend Micro specifically intended to induce infringement of the ‘114 patent. On information and belief, Trend Micro engaged in such inducement to promote the sales of the Trend Micro ‘114 Products, e.g., through Trend Micro user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘114 patent. Accordingly, Trend Micro has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary

way to infringe the ‘114 patent, knowing that such use constitutes infringement of the ‘114 patent.

225. The ‘114 patent is well-known within the industry as demonstrated by the over 39 citations to the ‘114 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Aigo Research Institute of Image Computing Co., Ltd. and General Electric Company). Several of Trend Micro’s competitors have paid considerable licensing fees for their use of the technology claimed by the ‘114 patent. In an effort to gain an advantage over Trend Micro’s competitors by utilizing the same licensed technology without paying reasonable royalties, Trend Micro infringed the ‘114 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

226. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘114 patent.

227. As a result of Trend Micro’s infringement of the '114 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Trend Micro’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Trend Micro together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff MOV Intelligence respectfully requests that this Court enter:

A. A judgment in favor of Plaintiff MOV Intelligence that HPE has infringed, either literally and/or under the doctrine of equivalents, the '230 patent, the '006 patent, the '516 patent, the '504 patent, and the '114 patent;

B. A judgment in favor of Plaintiff MOV Intelligence that Trend Micro has infringed, either literally and/or under the doctrine of equivalents, the '114 patent;

C. A judgment in favor of Plaintiff MOV Intelligence that HPE and F5 Networks have jointly infringed, either literally and/or under the doctrine of equivalents, the '418 patent;

D. An award of damages resulting from Defendants' acts of infringement in accordance with 35 U.S.C. § 284;

E. A judgment and order finding that Defendants' infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiff enhanced damages.

F. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees against Defendants.

G. Any and all other relief to which MOV Intelligence may show itself to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, MOV Intelligence requests a trial by jury of any issues so triable by right.

Dated: October 7, 2016

Respectfully submitted,

/s/ Dorian S. Berger _____

Elizabeth L. DeRieux (TX Bar No. 05770585)
D. Jeffrey Rambin (TX Bar No. 00791478)
CAPSHAW DERIEUX, LLP
114 E. Commerce Ave.
Gladewater, Texas 75647
Telephone: 903-845-5770
E-mail: ederieux@capshawlaw.com
E-mail: jrambin@capshawlaw.com

Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
BERGER & HIPSKIND LLP
1880 Century Park East, Ste. 815
Los Angeles, CA 95047
Telephone: 323-886-3430
Facsimile: 323-978-5508
E-mail: dsb@bergerhipskind.com
E-mail: dph@bergerhipskind.com

Attorneys for Marking Object Virtualization Intelligence, LLC